(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 44 11 449 C 1**

(51) Int. Cl.[6]:
B 60 R 25/00
B 60 R 25/04
E 05 B 49/00
G 09 C 1/00
G 06 F 12/14
H 04 L 9/00

(21) Aktenzeichen: P 44 11 449.4-51
(22) Anmeldetag: 1. 4. 94
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 16. 3. 95

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Mercedes-Benz Aktiengesellschaft, 70327 Stuttgart, DE

(72) Erfinder:
Brinkmeyer, Horst, Dr.-Ing., 71336 Waiblingen, DE; Daiss, Michael, 70794 Filderstadt, DE; Schwegler, Günter, 71384 Weinstadt, DE; Krüger, Bertolt, Dipl.-Math. Dr., 53113 Bonn, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:

DE 33 13 098 C1
DE 32 34 539 A1
DE 32 25 754 A1
DE 29 11 828 A1

Diebstahlschutz für das Auto, Temic Telefunken mikroelektronik GmbH, 8/93;
Ripe Integrity Primitives, Final report of RACE Integrity Primitives Evolution, 6/92, Port 3, Chapter 3, S. 67-109;

(54) Fahrzeugsicherungseinrichtung mit elektronischer Nutzungsberechtigungscodierung

(57) Es sind Fahrzeugsicherungseinrichtungen mit elektronischer Wegfahrsperre bekannt, bei denen die Codesicherung auf einem Wechselcodeverfahren oder einem symmetrischen Verschlüsselungsverfahren beruht. In beiden Fällen ist die Abspeicherung einer geheimen Codeinformation auf der Fahrzeugseite zwingend erforderlich.
Die neue Fahrzeugsicherungseinrichtung beinhaltet ein auf Basis einer Einwegfunktion arbeitendes Verschlüsselungsverfahren, bei dem nur schlüsselseitig die Abspeicherung geheimer Codeinformationen zwingend erforderlich ist, und zwar in Form von unterschiedlichen Urbildwerten einer Einwegfunktion, während fahrzeugseitig nur die Einwegfunktionswerte zu diesen Urbildwerten vorhanden zu sein brauchen, deren Auslesen aufgrund der praktischen Nichtumkehrbarkeit der Einwegfunktion keine unberechtigte Herstellung eines Nachschlüssels ermöglicht.
Verwendung bei der Realisierung von elektronisch ansteuerbaren Schließanlagen und/oder elektronischen Wegfahrsperren.

DE 44 11 449 C1

DE 44 11 449 C1

Beschreibung

Die Erfindung bezieht sich auf eine Fahrzeugsicherungseinrichtung mit elektronischer Nutzungsberechtigungscodierung nach dem Oberbegriff des Patentanspruchs 1.

Derartige Fahrzeugsicherungseinrichtungen sind z. B. als nach einem sogenannten Wechselcodeverfahren arbeitende elektronische Wegfahrsperren zum Schutz vor einer unberechtigten Fremdnutzung des Fahrzeugs bekannt, siehe z. B. den Firmenprospekt "Diebstahlschutz für das Auto" der Firma TEMIC TELEFUNKEN microelektronik GmbH vom August 1993. Gegenüber früher gebräuchlichen Festcodeverfahren, wie es beispielsweise in der Offenlegungsschrift DE 29 11 828 A1 beschrieben ist, ist bei derartigen Wechselcodeverfahren die Sicherheit gegenüber einer unberechtigten Fahrzeugbenutzung nach Abhören eines oder mehrerer Codesendeprotokolle dadurch erhöht, daß die Codeinformation bei jedem sogenannten Authentikationsvorgang, d. h. bei jedem Prüfvorgang der Nutzungsberechtigung, wechselt. Dieser Codewechsel läßt sich unter Beibehaltung der vom Festcodeverfahren her bekannten unidirektionalen Codeinformationsübertragung nur von der Schlüssel- zur Fahrzeugseite dadurch realisieren, daß sowohl auf der Schlüssel- wie auch auf der Fahrzeugseite eine geheime Basiszahlinformation und ein Algorithmus abgelegt werden, nach welchem die aufeinanderfolgenden Codeinformationen aus der Basiszahl ableitbar sind, so daß fahrzeugseitig durch jeweiligen Vergleich der fahrzeugseitig erzeugten Codeinformation mit der schlüsselseitig gesendeten Codeinformation die Benutzerberechtigung geprüft werden kann. Alternativ ist es bekannt, in die Schlüssel- und die Fahrzeugseite nach jeder erfolgreichen Authentikation jeweils eine neue, zufällig ausgewählte oder deterministisch festgelegte berechtigende Codeinformation für die nächste Authentikation einzubringen, siehe z. B. die Offenlegungsschrift DE 32 34 539 A1 und die Patentschrift DE 33 13 098 C1. Eine derartige Zwangssynchronisation erfordert allerdings einen drahtlos oder über elektrisch leitenden Kontakt zwischen Schlüsseleinheit und einer beteiligten Fahrzeuggeräteeinheit ermöglichten bidirektionalen Datenaustausch.

Neben den während einer Authentikation mit unidirektionaler Datenübertragung arbeitenden Wechselcodeverfahren sind des weiteren sogenannte symmetrische Verschlüsselungsverfahren bekannt, bei denen die Authentikation über bidirektionalen Datenaustausch erfolgt, wobei einerseits auf der Schlüsselseite und andererseits auf der Fahrzeugseite jeweils ein gleichartiger, geheimer Codieralgorithmus abgelegt ist. Dieser Algorithmus erzeugt auf eine beiden Seiten zugeführte Eingangsinformation, z. B. einer Zufallszahlinformation, hin eine jeweilige Codeinformation, wobei anschließend die schlüsselseitige Codeinformation zur Fahrzeugseite gesendet und dort mit der fahrzeugseitig erzeugten Codeinformation auf Übereinstimmung geprüft wird. Ein Verfahren dieser Art ist in der Offenlegungsschrift DE 32 25 754 A1 beschrieben.

Sämtliche der obigen bekannten Verfahren erfordern mithin die Speicherung einer geheimen Information auf der Fahrzeugseite. Dadurch besteht nicht nur eine gewisse Gefahr eines unberechtigten Auslesens dieser geheimen Information aus der Fahrzeugseite, sondern es muß außerdem für ein geschütztes fahrzeugseitiges Einbringen derartiger geheimer Dateninformationen gesorgt werden, was einen entsprechenden logistischen

Sicherheitsaufwand beim Fahrzeughersteller und in Werkstätten, in welchen diese geheime fahrzeugspezifische Information in Austauschgeräteeinheiten einzubringen ist, erfordert.

Der Erfindung liegt als technisches Problem die Bereitstellung einer Fahrzeugsicherungseinrichtung der eingangs genannten Art zugrunde, die bei verhältnismäßig geringem Aufwand, insbesondere bereits durch unidirektionale Datenübertragung, und komfortabler Bedienung einen relativ hohen Schutz vor unberechtigter Fremdnutzung des Fahrzeugs bietet, wobei es einem Unberechtigten insbesondere nicht möglich ist, einfach durch Abhören eines Authentikationsvorgangs oder Auslesen einer fahrzeugseitigen Codeinformation das Fahrzeug anschließend durch erfolgreiche Authentikation unter Benutzung der abgehörten oder ausgelesenen Informationen unberechtigt zu nutzen und wobei fahrzeugseitig keine geheimen Informationen abgelegt sein brauchen.

Dieses Problem wird durch eine Fahrzeugsicherungseinrichtung mit den Merkmalen des Patentanspruchs 1 gelöst. Die Fahrzeugsicherungseinrichtung bietet bei vergleichsweise geringem Aufwand einen verhältnismäßig hohen Schutz gegen unberechtigte Fremdnutzung des Fahrzeugs. Insbesondere ist eine fahrzeugseitige Einspeicherung einer geheimen Information nicht zwingend erforderlich, was sicherheitslogistischen Aufwand beim Fahrzeughersteller und in den Werkstätten erspart und damit verbundene Sicherheitsrisiken vermeidet und außerdem zur Folge hat, daß sich durch Auslesen der fahrzeugseitig untergebrachten Codeinformationen keine Nachschlüssel herstellen lassen, mit denen eine erfolgreiche Authentikation möglich ist. Der Wegfall von sicherheitslogistischen Maßnahmen fällt insbesondere dann merklich ins Gewicht, wenn zur Authentikation fahrzeugseitig eine Vielzahl von Geräteeinheiten beteiligt ist, um eine Umgehung der Wegfahrsperre durch einfachen Austausch einer oder einiger weniger authentikationsbeteiligter Geräteeinheiten unökonomisch zu machen. Die Codesicherheit der Authentikation beruht auf der definitionsgemäßen Eigenschaft einer mathematischen Einwegfunktion, daß nämlich der Algorithmus zur Berechnung eines Einwegfunktionswertes zu einem Urbildwert vergleichsweise einfach ist, hingegen die Gewinnung eines zu einem gegebenen Einwegfunktionswert gehörigen Urbildwertes nicht mit praktisch realisierbarem Rechenaufwand innerhalb einer zur Verfügung stehenden Zeitspanne möglich ist. Die Eigenschaft einer Funktion, eine Einwegfunktion zu sein, hängt daher auch von der vorhandenen Rechnerkapazität ab. Beim derzeitigen Stand der Rechnertechnologie sind derartige Einwegfunktionen z. B. in Form sogenannter Hashfunktionen bekannt, die vor allem zur Nachrichtensicherung in der Kryptographie Verwendung finden, wobei als Obergrenze für den praktisch beherrschbaren Rechenaufwand heutzutage eine Anzahl von ca. 2^{50} Berechnungs- und Speichervorgängen von Hashwerten angenommen werden kann. Aufgrund der praktischen Nichtumkehrbarkeit der Einwegfunktion brauchen die Einwegfunktionswerte fahrzeugseitig nicht geheim behandelt zu werden, denn selbst ein unberechtigtes Auslesen derselben aus dem Fahrzeug würde einen Unberechtigten nicht in die Lage versetzen, die zugehörigen Urbildwerte aufzufinden und damit einen elektronischen Nachschlüssel anzufertigen. Die Sicherheit des Systems gegen Ausnutzen eines Abhörens eines Authentikationsversuchs ist dadurch gegeben, daß für jeden Authentikationsversuch eine neue Urbildwert-

Codeinformation gesendet wird. Abhängig vom Ergebnis des Vergleichs von Ist- und Soll-Berechtigungsinformation gibt die fahrzeugseitige Authentikationseinheit eine Nutzungsfreigabeinformation ab, die bei positivem Authentikationsversuch zur Entschärfung einer zugehörigen elektronischen Wegfahrsperre und bei negativem Authentikationsversuch zu deren bleibender Schärfung führt, wobei die elektronische Wegfahrsperre beinhaltet, daß nach Abziehen des Zündschlüssels wenigstens eine fahrzeugseitige, für den Zugang zum Fahrzeug oder für den Betrieb des Fahrzeugs relevante Geräteeinheit, z. B. eine Schließsteuerung, ein Motorsteuergerät etc., in einer Blockierstellung gehalten wird.

Eine Ausgestaltung der Erfindung nach Anspruch 2 realisiert in vorteilhafter, einfacher Weise die Bereitstellung der schlüsselseitig abgelegten Urbildwerte, indem diese Wertefolge durch Hintereinanderausführung der Einwegfunktion gebildet wird, wonach sie im laufenden Schlüsselbetrieb rückwärts, d. h. vom zuletzt bestimmten bis zum anfänglichen Urbildwert ausgelesen wird. Fahrzeugseitig bringt dies den speichertechnischen Vorteil, daß nicht sämtliche zu den Urbildwerten gehörige Einwegfunktionswerte abgespeichert zu werden brauchen. Vielmehr genügt zur Bereitstellung der Soll-Berechtigungsinformation die anfängliche Abspeicherung des zu dem ersten gesendeten Urbildwert gehörigen Einwegfunktionswertes, wonach diese Speicherinformation jeweils bei einer erfolgreichen Authentikation mit derselben Schlüsseleinheit mit der für diese Authentikation gesendeten Urbildwertinformation überschrieben wird, da ein zuvor gesendeter Urbildwert stets gerade der Einwegfunktionswert des nachfolgend gesendeten Urbildwertes ist.

Mit einer Ausgestaltung der Erfindung nach Anspruch 3 läßt sich auf der Schlüsselseite Speicherplatz einsparen, indem nicht sämtliche, über die Lebensdauer der Schlüsseleinheit benötigte Urbildwerte, sondern lediglich Stützstellen in ausgewählten Abständen der gesamten Urbildwertfolge sowie ein jeweils aktueller Wertebereich zwischen zwei Stützstellen abgespeichert gehalten sind. Mit Hilfe des auch auf der Schlüsselseite abgelegten Einwegfunktionsalgorithmus läßt sich immer dann, wenn ein aktueller Bereich bis auf einen vorgebbaren Rest verbraucht ist, von der nächsten Stützstelle aus ein neuer aktueller Bereich durch rekursive Anwendung der Einwegfunktion generieren und abspeichern.

Durch eine Ausgestaltung der Erfindung nach Anspruch 4 ist fahrzeugseitig ein sogenannter Fangbereich gebildet, der es in einem vorgebbaren Umfang ermöglicht, die Fahrzeugseite wieder mit der Schlüsselseite zu synchronisieren, wenn die Synchronisation aufgrund einer oder mehrerer Sendeaktivitäten auf der Schlüsselseite, denen keine fahrzeugseitige Empfangsaktivität gegenüberstand, verlorengegangen ist. Entspricht der Einwegfunktionswert eines empfangenen Urbildwertes als Ist-Berechtigungsinformation nicht der momentanen fahrzeugseitigen Soll-Berechtigungsinformation, so wird durch den Fangbereich für eine vorgegebene maximale Anzahl von Wiederholungen das Durchlaufen einer rekursiven Einwegfunktionsbildung zugelassen, wobei der jeweils aus der bisherigen Ist-Berechtigungsinformation erzeugte Einwegfunktionswert als neue Ist-Berechtigungsinformation dient. Wenn mit einer derart neu bestimmten Ist-Berechtigungsinformation innerhalb des Fangbereichs Übereinstimmung mit der fahrzeugseitig gespeicherten Soll-Berechtigungsinformation erkannt wird, wird dies als positiver Authentikationsversuch gewertet, und demgemäß wird dann die Wegfahrsperre aufgehoben sowie die gesendete Urbildwertinformation als neue Soll-Berechtigungsinformation für den nächsten Authentikationsversuch mit diesem Schlüssel abgespeichert. Wird der Fangbereich so groß gewählt wie die Mächtigkeit einer insgesamt möglichen Urbildwertsequenz in der Schlüsseleinheit, so ermöglicht dies zudem ein vorteilhaft einfaches Einbinden eines berechtigenden Ersatzschlüssels bei gleichzeitigem automatischem Ungültigwerden des ersetzten Schlüssels. Dazu kann der Ersatzschlüssel bevorzugt durch eine Weiterbildung nach Anspruch 5 initialisiert werden, wofür lediglich die Abspeicherung eines einzigen geheimen Startwertes zur Einwegfunktionswertbildung für die Initialisierung des ersten und aller weiteren, den vorigen bei Bedarf sukzessive ersetzenden Schlüssel in einer Schlüsselzentrale nötig ist.

Als Einwegfunktion ist gemäß Anspruch 6 eine der aus der Kryptographie bekannten Hash-Funktionen, speziell eine RIPEMD-Algorithmus, verwendbar, wofür nach dem heutigen Stand der kryptographischen Wissenschaft die geforderte Einwegfunktionseigenschaft angenommen werden kann.

In Ausgestaltung der Erfindung nach Anspruch 7 sind mehrere fahrzeugseitige Geräteeinheiten parallel in die Authentikation einbezogen, wofür sie günstigerweise über einen gemeinsamen Datenbus verbunden sein können. Diese dezentrale Verteilung der Authentikation, die sich über alle fahrzeugrelevanten Geräteeinheiten erstrecken kann, erschwert wesentlich eine Umgehung der Wegfahrsperre durch mechanische Manipulationen in Form eines Geräteaustauschs, da dann alle diese von der Authentikation und der Wegfahrsperre betroffenen Geräteeinheiten ausgetauscht werden müßten, um das Fahrzeug für einen Unberechtigten nutzbar zu machen, der nicht über die Möglichkeit einer erfolgreichen Authentikation verfügt. Die einbezogenen Geräteeinheiten, insbesondere Steuergeräte der Fahrzeugelektronik, können dabei so ausgewählt sein, daß deren Austausch einen im Verhältnis zum gewonnenen Nutzen unverhältnismäßig hohen Aufwand bedeutet und daher uninteressant wird.

Bei einer Ausgestaltung der Erfindung nach Anspruch 8 ist jedenfalls die Schließsteuerung des Fahrzeugs in die Authentikation einbezogen, so daß sich das Fahrzeug ohne berechtigte Authentikation nicht nur nicht starten, sondern auch nicht ohne gewaltsame Manipulation öffnen läßt. Sind weitere Geräteeinheiten beteiligt, können diese beispielsweise durch einen Datenbus untereinander und mit der Schließsteuerung verbunden sein, wobei dann ein einziger fahrzeugseitiger Empfänger für die schlüsselseitig gesendeten Daten ausreicht, der beispielsweise der Schließsteuerung zugeordnet sein kann.

Eine Ausgestaltung der Erfindung nach Anspruch 9 hat den Vorteil, daß durch die anfängliche Identifizierungsprüfung bezüglich des Fahrzeugs und des Schlüssels erst einmal festgestellt wird, ob legitimierte Hardware-Einheiten miteinander in Verbindung stehen, bevor der eigentliche Authentikationsvorgang durchgeführt wird. So läßt sich die unnötige Aktivierung von Authentikationsoperationen, die wegen unrichtiger Schlüssel-Fahrzeug-Kombination nicht zum Erfolg führen können, vermeiden.

Eine Ausgestaltung der Erfindung nach Anspruch 10 erlaubt die Verwendung eines Schlüsselsatzes mit mehreren Schlüsseln für das Fahrzeug in schaltungstechnisch vorteilhafter Weise und unter Beibehaltung des

Einwegfunktions-Codieralgorithmus.

Eine bevorzugte Ausführungsform der Erfindung ist in der Zeichnung dargestellt und wird nachfolgend beschrieben.

Die einzige Figur zeigt ein Blockdiagramm einer Fahrzeugsicherungseinrichtung mit elektronischer Nutzungsberechtigungsprüfung mittels unidirektionaler Codedatenübertragung.

Die Fahrzeugsicherungseinrichtung beinhaltet benutzerseitig mehrere, z. B. acht, elektronische Schlüssel 1, von denen stellvertretend einer gezeigt ist, sowie fahrzeugseitig eine Mehrzahl von in die Nutzungssicherung einbezogenen Geräteeinheiten 2, von denen eine eine Schließsteuerung ist, deren Aufbau stellvertretend für die übrigen Geräteeinheiten in der Figur dargestellt ist, während die übrigen Geräteeinheiten die sonstigen Steuergeräte der fahrzeugelektrischen Anlage sind. Dabei ist der in der Figur auf der Fahrzeugseite links von der rechten punktierten Trennlinie dargestellte Schaltungsteil 2' nur in der Schließsteuerung vorhanden, während der rechts von dieser Trennlinie befindliche Schaltungsteil 2'' für alle einbezogenen Geräteeinheiten in identischer Form vorhanden ist. Sämtliche in die Sicherung einbezogenen Geräteeinheiten 2 kommunizieren in nicht gezeigter Weise über einen CAN-Bus, alternativ über eine andere Datenaustauschverbindung im Fahrzeug, untereinander sowie mit dem nur in der Schließsteuerung vorhandenen empfangsseitigen Schaltungsteil 2'. Schlüssel- und Geräteeinheiten 1, 2 sind dabei jeweils mit einem Prozessorchip bestückt, in denen die in der Figur jeweils in Blockform illustrierten und nachfolgend beschriebenen Funktionseinheiten weitgehend softwaremäßig implementiert sind.

Die Schlüsseleinheiten 1 besitzen jeweils einen Sender 5, mit dem schlüsselseitige Daten codiert über eine Infrarotstrecke 9 unidirektional zur Fahrzeugseite gesendet werden können, wo sie von einem Empfänger 10 im Eingangsschaltungsteil 2' der Schließsteuerung 2 empfangen und anschließend decodiert werden können. Jede Schlüsseleinheit 1 besitzt des weiteren eine Einheit 7 zur rekursiven Erzeugung von Einwegfunktionswerten einer z. B. in der Kryptographie verwendeten Hashfunktion H, wobei hier speziell als Hash-Einwegfunktion die aus "Ripe Integrity Primitives, Final report of RACE Intergrity Primitives Evaluation (R1040) (June 1992) Part III Recommended Integrity Primitives, Chapter 3 RIPEMD, S. 67—109" bekannte RIPEMD-Funktion verwendet ist. Eine Einwegfunktion ist hierbei als eine mathematische Funktion definiert, für die der Funktionswert eines gegebenen Urbildes aus ihrem Definitionsbereich eindeutig und vergleichsweise einfach bestimmbar ist, während es selbst mit in der Praxis maximal zur Verfügung stehendem Rechenaufwand nicht möglich ist, zu einem gegebenen Einwegfunktionswert einen Urbildwert zu finden. Die Bitlänge eines RIPEMD-Funktionswertes beträgt 16 Byte, wobei es für den vorliegenden Zweck der Fahrzeugsicherung ausreicht, den 16-Byte-Wert durch einen geeigneten Algorithmus in einen verkürzten 8-Byte-Wert zu transformieren, um Speicherplatz einzusparen. Mit dieser Hashfunktionswert-Erzeugungseinheit 7 werden durch wiederholtes Anwenden der Hashfunktion beginnend mit einem Startwert m_0 eine Anzahl n von Werten erzeugt und als Urbildwerte in einem Urbildwertspeicher 3 abgelegt, der über einen Zähler 21 rückwärts, d. h. beginnend mit dem letzten Wert m_{n-1} der Urbildwertsequenz $m_0, \ldots, m_{n-1}$ sukzessive in einen Zwischenspeicher 4 auslesbar ist. Die Anzahl n bestimmt die Anzahl der durch die Schlüsseleinheit 1 während ihrer Lebensdauer maximal auslösbaren Authentikationsversuche und ist entsprechend zu wählen, z. B. $n = 100\,000$ für ca. 20 Schlüsselbetätigungen täglich bei ca. 10 Jahren Schlüssellebensdauer. Der Zwischenspeicher 4 ist über ein Startsignal S_{ST} auslesesteuerbar, das mittels einer Benutzertaste 6 generiert wird.

Zur Abspeicherung von Hardware-Identifikationsdaten, die eine fahrzeugspezifische sowie eine schlüsselspezifische Information umfassen, weist jede Schlüsseleinheit 1 einen Identifikationsdatenspeicher 8 auf, dessen Daten die Schlüsseleinheit 1 mit der jeweils aus dem Zwischenspeicher 4 kommenden Urbildwertinformation m_i zu der als Nachricht zu sendenden Benutzercodeinformation M verknüpft.

Fahrzeugseitig beinhaltet der informationseingangsseitige Schaltungsteil 2' der Schließsteuerung 2 außer dem Empfänger 10 einen Identifikationsdatenspeicher 11, einen Identifikationsdatenvergleicher 12 sowie eine Gatterfunktion 13, jeweils in Software-Realisierung. Der Komparator 12 vergleicht die in diesem Schließsteuergerät-Schaltungsteil 2' aus der empfangenen Benutzercodeinformation M extrahierte Identifikationsdateninformation ID_S mit der in dem fahrzeugseitigen Identifikationsdatenspeicher 11 abgelegten Identifikationsdateninformation ID_K und beaufschlagt mit seinem Ausgangssignal einen Steuereingang des Gatters 13, dessen anderer Eingang vom Benutzercodeinformationssignal M beaufschlagt wird. Wahlweise kann an die Schließsteuerung 2 eine Diagnoseschnittstelle 19 angeschlossen werden, wie in der Figur punktiert angedeutet ist.

Der rechts von der rechten punktierten Trennlinie in der Figur gezeigte Schließsteuerungs-Schaltungsteil 2'', der auch in allen anderen, in das Fahrzeugsicherungssystem einbezogenen Geräteeinheiten 2 in identischer Form vorhanden ist, beinhaltet, wiederum softwarerealisiert, eine Einheit 14 zur Hash-Funktionswertberechnung sowie eine Gatterfunktion 15, denen beiden die jeweils in der Benutzercodeinformation M enthaltene Urbildwertinformation m_i zuführbar ist. Der Ausgang dieses Gatters 15 ist mit einem Soll-Berechtigungsinformationsspeicher 16 mit einer der Anzahl von Schlüsseleinheiten 1 entsprechenden Speicherstellenanzahl verbunden, wobei die einzelnen Speicherstellen abhängig von der erkannten Schlüsselidentität ID_j, d. h. der Schlüsselnummer, ansprechbar sind. Der Ausgang dieses Speichers 16 wiederum ist mit einem Eingang eines Komparatorblocks 17 verbunden, dem über einen weiteren Eingang das Ausgangssignal m' der Hash-Funktionswerterzeugungseinheit 14 zuführbar ist. Dieses Ausgangssignal (m') ist außerdem einem weiteren Gatterblock 18 zugeführt, dessen Steuereingang von einem Nichtübereinstimmungssignal N_U des Komparators 17 beaufschlagt wird. Bei erkannter Übereinstimmung erzeugt hingegen der Komparator 17 ein Nutzungsfreigabesignal S_F zum Aufheben eines die Software-Betriebsbereitschaft der betreffenden Geräteeinheit 2 blockierenden Zustandes, der Teil einer alle diese Geräteeinheiten blockiert haltenden elektronischen Wegfahrsperre ist. Das Nutzungsfreigabesignal S_F, das eine erfolgreiche Authentikation, d. h. Nutzungsberechtigungsprüfung, repräsentiert, verläßt dabei nicht die zugehörige Geräteeinheit und vorzugsweise nicht einmal den Chipbereich, was eine hohe Sicherheit gegen unbefugte Fremdeinspeisung der Nutzungsfreigabeinformation bietet, und ist außerdem als Steuersignal dem mit der gesendeten Urbildwertinformation m_i beaufschlagten

Gatterblock 15 zugeführt, um ein Abspeichern dieser Information als neue Soll-Berechtigungsinformation zu ermöglichen. Zur Durchführung von Sonderfunktionen über die ggf. an die Schließsteuerung angeschlossene Diagnoseschnittstelle 19 oder eine Schlüsseleinheit 1 ist bei Bedarf ein zusätzlicher Sonderfunktions-Sollberechtigungsinformationsspeicher 20 parallel zu dem normalen Soll-Berechtigungsinformationsspeicher 16 vorgesehen, wie in der Figur gestrichelt angedeutet.

Wie oben erwähnt, sind alle in den Authentikationsvorgang einbezogenen Geräteeinheiten 2 gleichzeitig auch in eine elektronische Wegfahrsperre einbezogen, die durch Abstellen der Zündung jeweils geschärft wird und durch einen nachfolgenden erfolgreichen Authentikationsvorgang wieder entschärfbar ist. Da in allen diesen Geräteeinheiten 2 dieselben Authentikationsoperationen durchgeführt werden, werden alle diese Einheiten 2 bei einer berechtigten Nutzungsanforderung gleichzeitig wieder betriebsbereit, während bei einer unberechtigten Nutzungsanforderung wenigstens eine gesperrt bleibt. Die Verteilung des Authentikationsvorgangs auf alle diese Fahrzeuggeräteeinheiten und die korrespondierende Sperrung derselben hat den Vorteil, daß sich das Fahrzeug nicht durch einfachen Austausch einer oder einiger weniger Geräteeinheiten unter Umgehung der Authentikationsnotwendigkeit weiterbenutzen läßt. Vielmehr müßten alle diese Geräteeinheiten ausgetauscht werden, was mit so hohem Kostenaufwand verbunden ist, daß ein derartiger Versuch einer unberechtigten Fremdnutzung uninteressant ist.

Nachfolgend wird im Detail auf die Funktionsweise der wie oben beschrieben aufgebauten Fahrzeugsicherungseinrichtung eingegangen.

Der Gesamtablauf beginnt zunächst vor der Fahrzeuginbetriebnahme mit den nötigen Initialisierungsvorgängen beim Schlüsselhersteller bzw. einer für diesen Zweck eingerichteten Schlüsselzentrale SH. Dort wird zunächst für jeden Schlüssel individuell ein geheimer Zufallswert r_0 erzeugt. Aus diesem wird dann durch mehrfaches, z. B. 400 000faches, aufeinanderfolgendes Anwenden der Hashfunktion der geheime Urbildstartwert m_0 berechnet und in die jeweilige Schlüsseleinheit 1 in den Urbildwertspeicher 3 eingebracht. Die zunächst nicht verwendeten Hashfunktionswerte zwischen dem geheimen Anfangszufallswert r_0 und dem Urbildstartwert m_0 können als Hilfsmittel für einen weiter unten beschriebenen Schlüsselersatz dienen, wozu der zugehörige Anfangszufallswert r_0 in einem geschützten Speicher der Schlüsselzentrale SH aufbewahrt wird. Neben dem Urbildstartwert m_0 werden bei der Produktion der Schlüsseleinheit 1 auch die Identifikationsdaten ID_S in den zugehörigen Speicher 8 eingebracht, wobei diese Daten neben fahrzeugspezifischen Daten auch eine Schlüsselnummer enthalten, welche die für ein Fahrzeug gleichzeitig gültigen Schlüsseleinheiten voneinander unterscheidet. Bis auf die Schlüsselnummer sind die Identifikationsdaten der für ein Fahrzeug gleichzeitig gültigen Schlüsseleinheiten 1 gleich und bilden folglich eine Art Schlüsselsatznummer. Parallel werden die identischen Identifikationsdaten von der Schlüsselzentrale SH zum Einspeichern in den zugehörigen Speicher 11 der Schließsteuerung zur Verfügung gestellt. Weiter werden in der Schlüsselzentrale SH bei der Initialisierung ausgehend von dem Urbildstartwert m_0 die nächsten n rekursiven Hash-Funktionswerte $H^j m_0$; $J = 1, \ldots, n-1$ vorausberechnet und der erhaltene Endwert m_n als schlüsselspezifischer Soll-Berechtigungsinformationsstartwert zur fahrzeugseitigen Initialisierung der zugehörigen Speicherstelle der jeweiligen Soll-Berechtigungsinformationsspeicher 16 zusammen mit den Identifikationsdaten an den Fahrzeughersteller übergeben.

Mit den von der Schlüsselzentrale SH erhaltenen Initialisierungsdaten erfolgt die fahrzeugseitige Initialisierung durch den Fahrzeughersteller zunächst durch Einbringen eines fahrzeugspezifischen Hash-Funktionswertes, der zu einer ebenfalls in der Schlüsselzentrale SH erzeugten Hash-Funktionswertfolge gehört, in den Sonder-Hashfunktionswertspeicher 20, und zwar je nach Sicherheitsanforderung zum Abschluß der Produktion beim Fahrzeughersteller oder beim Geräteeinbau am Band bzw. in der Werkstatt. Zur Initialisierung der Soll-Berechtigungsinformationsspeicher 16 wird im Verlauf der Produktion jede einer bestimmten Schlüsseleinheit 1 zugeordnete Speicherstelle dieser Speicher 16 aller beteiligten Geräteeinheiten 2 mit dem von der Schlüsselzentrale SH hierfür schlüsselspezifisch zur Verfügung gestellten Startwert m_n geladen. Hierzu muß sich die Bedienperson über die Diagnoseschnittstelle 19 über den fahrzeugspezifisch im Sonderfunktionsspeicher 20 abgelegten Hash-Funktionswert authorisieren, bevor sie die Anfangsinitialisierung durch Überschreiben des Anfangswertes null mit dem schlüsselspezifischen Soll-Berechtigungsinformationsanfangswert m_n vornehmen kann, wobei die Speicherstellen der Soll-Berechtigungsinformationsspeicher 16 gegen normales Überschreiben geschützt werden, solange sie den Wert null beinhalten. Der Sonderfunktionsspeicher 20 dient dabei als Transportschutz für die Geräteeinheiten, kann jedoch je nach Bedarf die Ausführung weiterer Sonderfunktionen ermöglichen. Sichergestellt werden muß bei dieser Geräteinitialisierung, daß die Nullwerte aller Speicherstellen für die verschiedenen Schlüssel eines Satzes überschrieben werden, um eine spätere unberechtigte Fremdinitialisierung zu verhindern. Alternativ ist es möglich, den Soll-Berechtigungsinformationsstartwert m_n mit einer ersten Schlüsselbetätigung auf die Fahrzeugseite zur Initialisierung zu übergeben. Im Fall eines Reparaturaustauschs einer beteiligten Geräteeinheit 2 kann zudem vorgesehen sein, die neu eingesetzte Einheit über den CAN-Bus mit den Startwerten, die in den anderen Einheiten vorliegen, zu initialisieren, was automatisch das Überschreiben sämtlicher Startwerte null sicherstellt. Zur Unterscheidung, ob die einer Geräteeinheit 2 zugeführte Information M eine normale Authentikation oder eine Sonderfunktionsoperation beinhaltet, enthält die zugeführte Information M neben den Identifikationsdaten, die ca. 8 Byte umfassen, und der auf 8 Byte verkürzten Urbildwertinformation zusätzlich einen Funktionscode, für den eine Datenlänge von 1 Byte ausreichend ist.

Nach erfolgter Initialisierung generiert jede Schlüsseleinheit 1 mit dem erstmaligen Anschließen an die Energieversorgung über ihre Hashfunktionswert-Erzeugungseinheit 7 aus dem abgelegten Startwert m_0 die übrigen n-1-Werte durch n-1malige, wiederholte Anwendung der Hashfunktion auf den jeweils zuvor erhaltenen Funktionswert und speichert die erhaltene Wertefolge als Urbildwertefolge im entsprechenden Speicher 3 zum sukzessiven Rückwärtsauslesen ab, wobei der zugehörige Zähler 21 anfangs auf den Wert n-1 gesetzt ist und sich bei jeder Betätigung der Aktivierungstaste 6 um eins verringert. Da die Speicherung dieser beispielsweise 100 000 16-Byte-Werte entsprechenden Speicherbedarf erfordert, ist folgendes, speicherplatzsparendes Alternativvorgehen möglich. Es werden ausgewählte Werte der erzeugten Hash-Funktionswertfolge m_0 bis

m_{n-1}, z. B. nur jeder hundertste Wert, im Speicher 3 als Stützstellen fest abgespeichert. Zusätzlich wird jeweils ein aktuell anstehender Abschnitt der Wertesequenz m_0 bis m_{n-1} zwischen zwei Stützstellen, der z. B. aus jeweils 100 Werten besteht, im Speicher 3 abgelegt, so daß auf diese Weise zu jedem Zeitpunkt nur 1100 8-Byte-Werte im Speicher 3 gehalten werden müssen. Sobald durch laufende Schlüsselbenutzung das Ende eines aktuellen Wertefolgenabschnitts erreicht ist, wird mit der nächsten Stützstelle als Eingangsinformation die Hash-Funktionswertbildung 7 zur Erzeugung des nächstfolgenden Wertefolgenabschnitts zwischen zwei Stützstellen aktiviert, woraufhin der verbrauchte Wertefolgenabschnitt durch den neu berechneten überschrieben wird. Dabei ist vom Gesichtspunkt geringen Speicherbedarfs eine gleichgroße Speicheraufteilung für die Stützstellen und den Bereich zwischen zwei Stützstellen noch besser, wobei dann jeder Speicherteil eine ca. der Wurzel aus der Mächtigkeit n der gesamten Wertefolge m_0 bis m_{n-1} entsprechende Speicherstellenanzahl beinhaltet. Für den Fall geringstmöglicher Speicherbeanspruchung ist es als weitere Alternative möglich, nur den Anfangswert m_0 abgespeichert zu halten und nach jeder Schlüsselaktivierung ausgehend von diesem Startwert m_0 erneut eine wiederholte Hashfunktionswertbildung durchzuführen und diese Bildung sukzessive jeweils einmal weniger zu wiederholen sowie den jeweiligen Endwert dann direkt in den Zwischenspeicher 4 zu geben. Beliebige andere Aufteilungen sind gleichfalls möglich, z. B. logarithmische Stützstellenwahl.

Damit sind die vorbereitenden Operationen für die Aufnahme des normalen Authentikationsbetriebs mit der Fahrzeugsicherungseinrichtung abgeschlossen. Nachfolgend wird ein derartiger Authentikationsversuch, mit der sich ein Benutzer gegenüber dem Fahrzeug als nutzungsberechtigt auszuweisen und dadurch das Öffnen des Fahrzeugs sowie das Aufheben der beim Abstellen des Fahrzeugs geschärften Wegfahrsperre zu erreichen versucht, erläutert. Ein solcher Authentikationsvorgang wird durch Betätigen der Starttaste 6 einer Schlüsseleinheit 1 eingeleitet, wobei das damit erzeugte Startsignal S_{ST} das Auslesen des momentan im Zwischenspeicher 4 vorliegenden Urbildwertes m_i bewirkt, der anschließend zusammen mit den schlüsselseitigen Identifikationsdaten ID_S als Benutzercodeinformation M an den Sender 5 weitergeleitet und von dort über die Infrarotübertragungsstrecke 9 dem fahrzeugseitigen Empfänger 10 zugeleitet wird. Dort wird in der Schließsteuerung 2 zunächst die Identifikationsdateninformation ID_S aus der Benutzercodeinformation M extrahiert und mit den fahrzeugseitigen Identifikationsdaten ID_K verglichen. Liegt die dadurch geprüfte, geforderte Hardware-Identität eines für das Fahrzeug bestimmten Schlüssels 1 nicht vor, so wird mit einer entsprechenden Steuerinformation an dan Gatterfunktionsblock 13 die Weiterleitung der Benutzercodeinformation M auf den CAN-Bus und von dort an die weiteren Steuergeräteeinheiten verhindert, und der Authentikationsvorgang wird abgebrochen, ohne das Fahrzeug zu entriegeln oder die Wegfahrsperre aufzuheben. Andernfalls wird anschließend die Funktionscodeinformation daraufhin abgefragt, ob ein normaler Authentikationsvorgang oder ein Diagnosevorgang, z. B. zur Fehlerbehandlung, vorliegt.

Liegt ein normaler, identifikationsgeprüfter Authentikationsversuch vor, so wird der gesendete Urbildwert m_i als Teil der übertragenen Benutzercodeinformation M von der Schließsteuerung über den CAN-Bus an alle beteiligten Steuergeräte 2 und dort jeweils zur Hash-Funktionswerterzeugungseinheit 14 und zu dem Gatter 15 geleitet. Die Hash-Funktionswerterzeugungseinheit 14 berechnet den zum zugeführten Urbildwert m_i gehörigen Hash-Funktionswert m' und leitet diesen als Ist-Berechtigungsinformation m' an den Komparator 17 sowie an das zweite Gatter 18 weiter. Zwischenzeitlich wird anhand der in der Benutzercodeinformation M enthaltenen Identifikationsdaten ID_S die zugehörige Schlüsselnummer ID_j ermittelt und der in der zugehörigen Speicherstelle des Soll-Berechtigungsinformationsspeichers 16 gespeicherte Wert m_{i+1} an den anderen Eingang des Komparators 17 ausgelesen, wobei dieser Wert m_{i+1} der dem Steuergerät 2 bei der letztmalig mit dieser Schlüsseleinheit 1 erfolgreich durchgeführten Authentikation zugeführten Urbildwertinformation entspricht. Stellt der Komparator 17 Übereinstimmung von Ist- und Soll-Berechtigungsinformation fest $m' = m_{i+1}$, so erzeugt er das Nutzungsfreigabesignal S_F, das zum einen als an das Gatter 15 rückgeführtes Steuersignal das Überschreiben der betreffenden Speicherstelle durch den bei dieser Authentikation zugeführten Urbildwert m_i auslöst und zum anderen zusammen mit der simultan in den anderen beteiligten Steuergeräten erzeugten Nutzungsfreigabeinformation die gesamte Aufhebung der elektronischen Wegfahrsperre bewirkt, indem alle Steuergeräte wieder in ihren betriebsbereiten Zustand gebracht werden. Wenn in einigen Geräteeinheiten Speicherplatz eingespart werden soll, kann vorgesehen werden, in diesen nur einen Teil, z. B. 2 Byte, der gesamten Soll-Berechtigungsinformation m_{i+1} einzuspeichern und im Komparatorblock 17 nur diesen Teil mit dem entsprechenden Teil des Hash-Funktionswertes m' zu vergleichen. Um dennoch eine fehlerhafte Entschärfung der Wegfahrsperre auszuschließen, die ansonsten wegen des reduzierten Vergleichs besonders bei großem Fangbereich auftreten könnte, wird für mindestens eine Geräteeinheit, z. B. das Schließsteuergerät, der vollständige Codevergleich beibehalten, dessen Resultat den Geräten mit verkürztem Vergleich übermittelt wird, wobei die dortige Erzeugung der Nutzungsfreigabeinformation an das Vorliegen eines positiven Ergebnisses des vollständigen Codevergleichs gekoppelt wird.

Stellt der Komparator-Funktionsblock 17 hingegen eine Nichtübereinstimmung fest, so sendet er, vorausgesetzt, daß die Anzahl aufeinanderfolgender Nichtübereinstimmungen noch nicht den Fangbereich mit einer Anzahl N möglicher Wiederholungen überschritten hat, ein Nichtübereinstimmungssignal N_U an das Gatter 18, das daraufhin den geräteseitig erzeugten Hash-Funktionswert m' an die Eingangsseite der Hash-Funktionswerterzeugungseinheit 14 zurückleitet, woraufhin letztere mit diesem Eingangswert m' eine erneute Hash-Funktionswertbildung durchführt, deren Ergebnis dann als neue Ist-Berechtigungsinformation an den Komparator 17 gegeben wird. Diese rekursive Hash-Funktionswerterzeugung wird so lange fortgesetzt, bis entweder der Komparator 17 Übereinstimmung einer der nacheinander erzeugten Ist-Berechtigungsinformationen mit der vorliegenden Soll-Berechtigungsinformation m_{i+1} feststellt, wonach wie oben angegeben fortgesetzt wird, oder die Schleifenwiederholungsanzahl die durch den Fangbereich vorgegebene Maximalanzahl N, z. B. N = 100 000, erreicht hat, wonach der Authentikationsvorgang als unberechtigt unter Aufrechterhaltung der Wegfahrsperre abgebrochen wird, oder eine neue Benutzercodeinformation mit richtigen Identifikations-

daten ankommt, wonach der Schleifenzähler rückgesetzt und die Hash-Funktionswerterzeugung mit dem neu übertragenen Urbildwert fortgesetzt wird.

Wie bereits oben kurz ausgeführt, dient der Fangbereich dazu, eine durch eine oder mehrmalige Schlüsselbetätigung ohne Empfangskontakt der Fahrzeugseite für das zugehörige Sendeprotokoll außer Tritt geratene Synchronisierung von Schlüssel- und Fahrzeugseite dadurch wiederherzustellen, daß die Fahrzeugseite mittels einer entsprechend häufigen, aufeinanderfolgenden Hash-Funktionswertbildung innerhalb des Fangbereichs auf den inzwischen vorliegenden Urbildwert im Schlüssel 1 nachgestellt wird. Wenn der Fangbereich N gerade so groß gewählt ist wie die Mächtigkeit n der Urbildwertfolge, kann die Synchronisation für einen berechtigenden Schlüssel stets wiederhergestellt werden. Aufgrund der hashfunktionswerttypischen Eigenschaft, daß die Funktionswerte praktisch mit gleicher Wahrscheinlichkeit über den gesamten Wertebereich verteilt angenommen werden, und der Tatsache, daß selbst bei Verwendung eines reduzierten Algorithmus mit 8-Byte-Werten ca. 10^{20} Funktionswerte möglich sind, ist es auch bei einer Fangbereichgröße von $N = 10^5$ verschwindend unwahrscheinlich, daß ein Unberechtigter, selbst wenn er die Identifikationsprüfung auf irgendeine Weise bewältigt haben sollte, durch probeweises Senden von Urbildfunktionswerten unter Mithilfe des Fangbereiches eine positive Authentikation erreicht, wobei häufigere derartige Versuche ggf. durch ein entsprechendes Zeit- oder Versuchsanzahlfenster verhindert werden können, innerhalb welchem eine berechtigende Authentikation auftreten muß, während ansonsten die Fahrzeugnutzung gegenüber weiteren Authentikationsversuchen gesperrt bleibt, wobei eine derartige Sperre z. B. nur vom Fahrzeughersteller über die Diagnoseschnittstelle 19 entriegelbar ist. Es versteht sich, daß die Arbeitsweise der Fahrzeugsicherungseinrichtung analog für jeden beliebigen weiteren Authentifikationsvorgang derselben sowie anderer Schlüsseleinheiten wie oben beschrieben abläuft.

Die Wahl eines zur Mächtigkeit der Urbildwertfolge n gleichgroßen Fangbereichs $N = n$ ergibt des weiteren eine sehr komfortable Möglichkeit, einen Ersatzschlüssel anzufertigen. Wie oben erwähnt, wurde beim Schlüsselhersteller SH der Urbildstartwert m_0 durch oftmalige Hash-Funktionswertbildung aus einem schlüsselspezifischen Anfangszufallswert r_0 erzeugt, z. B. durch T-fache Anwendung, d. h. $m_0 = H^T(r_0)$, mit beispielsweise $T = 400\,000$. Soll nun ein Ersatzschlüssel bereitgestellt werden, wird er beim Schlüsselhersteller SH wie der ursprüngliche Schlüssel initialisiert, mit der Ausnahme, daß ausgehend vom gleichen Anfangszufallswert r_0 als Urbildstartwert m_0' der Wert $m_0' = H^{T-N}(r_0)$ gewählt wird. Nun wird mit diesem Ersatzschlüssel ein Authentikationsdialog mit dem Fahrzeug geführt. Der Ersatzschlüssel sendet dabei zuerst den Wert $x = H(m'_{n-1}) = H^{n-1}(m_0') = H^{T-1}(r_0)$ an das Fahrzeug. Dieser Wert liegt jedoch mit Sicherheit im Fangbereich der Fahrzeugseite, denn es folgt daraus, daß $H^N(x) = H^{T+N-1}(r_0) = H^{N-1}(m_0)$ ist. Der Ersatzschlüssel wird damit automatisch durch den erstmaligen Authentikationsdialog über den Fangbereich als berechtigender Schlüssel interpretiert, wodurch gleichzeitig der aktuell übermittelte Wert x in die fahrzeugseitigen Soll-Berechtigungsinformationsspeicher 16 übernommen wird. Dies macht wiederum gleichzeitig den ursprünglichen Schlüssel automatisch ungültig, da dessen Werte mit Sicherheit außerhalb des Fangbereichs des neuen Urbildwertes x liegen. Ein gesonderter Sperrvorgang für den ursprünglichen und beispielsweise verlorengegangenen Schlüssel ist damit unnötig. Mit dieser Vorgehensweise lassen sich eine Anzahl T/N von Ersatzschlüsseln nacheinander authentisieren, als konkretes Beispiel ergibt sich bei $T = 400\,000$ und $N = n = 100\,000$ eine Bereitstellung von vier nacheinander einsetzbaren Schlüsseln derselben Schlüsselnummer. Selbstverständlich ist je nach Bedarf zusätzlich eine Ersatzschlüsselimplementierung im Feld durch Verwendung eines zusätzlichen Verschlüsselungsverfahrens, beispielsweise des asymmetrischen, in der Kryptographie bekannten RSA-Signaturverfahrens (beschrieben in Annex C von ISO/IEC JTC1/SC20/WG N115, DIS 9594-8, Gloucester, Nov. 1987) oder des symmetrischen DES (data encryption standard)-Verfahrens, realisierbar, insbesondere wenn der Fangbereich kleiner als die Mächtigkeit der Urbildwertfolge gewählt wird und daher die obige Technik der Ersatzschlüsselimplementierung nicht möglich ist. Des weiteren kommt eine Ersatzschlüsselimplementierung über die Diagnoseschnittstelle 19 und den Sonderfunktionsspeicher 20 in Betracht.

Die gezeigte Fahrzeugsicherungseinrichtung stellt folglich eine wenig aufwendige und einen relativ hohen Schutz bietende Sicherung vor unberechtigter Fahrzeugfremdnutzung zur Verfügung, bei der insbesondere die geschützte Abspeicherung geheimer Codeinformationen auf der Fahrzeugseite entfallen kann, was die Einbeziehung einer Vielzahl von Fahrzeuggeräteeinheiten ohne sicherheitslogistische Probleme erlaubt. Außerdem ist eine aufwendige bidirektionale Datenkommunikation zwischen Schlüssel- und Fahrzeugseite nicht zwingend erforderlich. Speziell kann noch bemerkt werden, daß für den Hashfunktionscode 64 Bit ausreichen und daher die Übertragungszeit sowie der rechentechnische Aufwand deutlich geringer sind als bei einer ebenfalls denkbaren Verwendung des RSA-Verfahrens, das als ein asymmetrisches Verschlüsselungsverfahren ebenfalls nur eine einseitige Abspeicherung einer geheimen Information benötigt, jedoch eine hohe Wortlänge von 512 Bit hat und somit unter Berücksichtigung der bei einem Fahrzeug vorhandenen Rechenkapazitäten lange Rechen- und Übertragungszeiten erfordert.

Es versteht sich, daß zu obigem Beispiel nur die erfindungswesentlichsten Einheiten und Operationen erwähnt und daneben weitere, übliche Einheiten und Betriebsabläufe vorgesehen sind, und daß der Fachmann im Rahmen der Erfindung eine Vielzahl von Modifikationen dieser Ausführungsform vorzunehmen vermag, z. B. die Verwendung einer anderen Einwegfunktion, anwendungsspezifische Veränderungen der konkret angegebenen Zahlenbeispiele, Verzicht auf die Identifikationsprüfung und/oder auf die Sonderfunktionsmöglichkeit oder Verwendung eines Chipkartensystems anstelle der Infrarotsignalübertragung. Zudem kann die Erfindung als System mit bidirektionalem Authentikationsdatenaustausch realisiert sein, bei dem z. B. eine Zufallszahlinformation vom Fahrzeug zur Schlüsseleinheit gesendet und mit der Urbildwertinformation XOR-verknüpft rückübertragen und auf Übereinstimmung verglichen wird. Eine derartige Ausgestaltung verhindert, daß sich ein Unberechtigter, der während eines zeitweiligen Besitzes eines berechtigenden Schlüssels aufeinanderfolgende Benutzercodeinformationen aus selbigem angefertigt, mit diesem Nachschlüssel erfolgreich gegenüber dem Fahrzeug authentisieren kann.

Patentansprüche

1. Fahrzeugsicherungseinrichtung mit elektronischer Nutzungsberechtigungscodierung, mit
   - einer benutzerseitigen Schlüsseleinheit (1) zum aufeinanderfolgenden Senden voneinander verschiedener Benutzercodeinformationen (M),
   - einer fahrzeugseitigen Geräteeinheit (2) zum Empfangen der jeweils von einer Schlüsseleinheit gesendeten Benutzercodeinformation, zum Bestimmen einer von der empfangenen Benutzercodeinformation abhängigen Ist-Berechtigungsinformation (m') und Vergleichen derselben mit einer fahrzeugseitig vorliegenden Soll-Berechtigungsinformation (m_{i+1}) sowie zum vergleichsabhängigen Erzeugen einer Nutzungsfreigabeinformation (S_F),

dadurch gekennzeichnet, daß
   - die aufeinander folgenden gesendeten Benutzercodeinformationen (M) einen Urbildwert (m_i) für eine Einwegfunktion (H) beinhalten,
   - die Soll-Berechtigungsinformation (m_{i+1}) jeweils der Einwegfunktionswert ($m_{i+1} = H(m_i)$) des in einer zugehörigen Benutzercodeinformation enthaltenen Urbildwertes (m_i) ist und
   - die Bestimmung der Ist-Berechtigungsinformation (m') aus der empfangenen Benutzercodeinformation (M) die Bildung des Einwegfunktionswertes ($H(m_i)$) des in der empfangenen Benutzercodeinformation enthaltenen Urbildwertes (m_i) beinhaltet.

2. Fahrzeugsicherungseinrichtung nach Anspruch 1, weiter dadurch gekennzeichnet, daß
   - die aufeinanderfolgend gesendeten Urbildwerte eine Sequenz ($m_0, \ldots, m_{n-1}$) darstellen, die sich durch wiederholte Anwendung der Einwegfunktion (H) ergibt, wobei diese Urbildwerte in gegenüber der Sequenzbildung umgekehrter Reihenfolge zur Bildung der aufeinanderfolgenden Benutzercodeinformationen herangezogen werden, und
   - die Soll-Berechtigungsinformation jeweils aus demjenigen Urbildwert (m_{i+1}) besteht, der beim letztmalig mit dieser Schlüsseleinheit (1) positiv verlaufenden Nutzungsberechtigungs-Prüfvorgang mit der Benutzercodeinformation gesendet worden ist.

3. Fahrzeugsicherungseinrichtung nach Anspruch 2, weiter dadurch gekennzeichnet, daß ausgewählte Folgenglieder der Sequenz ($m_0, \ldots, m_{n-1}$) als Stützstellen sowie eine jeweils aktuelle Teilsequenz zwischen zwei Stützstellen in einem Urbildwertspeicher (3) der Schlüsseleinheit (1) abgespeichert sind, wobei spätestens dann jeweils eine nachfolgende aktuelle Teilsequenz erzeugt und anstelle der bisherigen abgespeichert wird, wenn der letzte Urbildwert der bisherigen Teilsequenz gesendet wurde.

4. Fahrzeugsicherungseinrichtung nach Anspruch 2 oder 3, weiter dadurch gekennzeichnet, daß nach jeweils negativem Ergebnis des Vergleichs von Ist- und Soll-Berechtigungsinformation für eine vorgegebene maximale Anzahl (N) von Wiederholungen eine neue Ist-Berechtigungsinformation als Einwegfunktionswert der bisherigen Ist-Berechtigungsinformation bestimmt und diese mit der Soll-Berechtigungsinformation verglichen wird.

5. Fahrzeugsicherungseinrichtung nach einem der Ansprüche 2 bis 4, weiter dadurch gekennzeichnet, daß für die Schlüsseleinheit (1) sukzessiv einsetzbare Ersatzschlüsseleinheiten vorgesehen sind, wobei die Urbildwerte einer nachfolgend benutzbaren Schlüsseleinheit eine unmittelbar vor der Urbildwertsequenz ($m_v, \ldots, m_{v+n-1}$) einer vorhergehenden Schlüsseleinheit liegende Teilsequenz ($m_{v-n}, \ldots, m_{v-1}$) einer ausgehend von einem schlüsselnummerspezifisch zentral abgespeicherten Startwert (r_0) durch wiederholte Einwegfunktionswertbildung ($H^T(r_0)$) erzeugten Gesamtsequenz ($r_0, \ldots, H^T(r_0)$) bilden.

6. Fahrzeugsicherungseinrichtung nach einem der Ansprüche 1 bis 5, weiter dadurch gekennzeichnet, daß als Einwegfunktion eine kryptographische Hash-Funktion, insbesondere die RIPEMD-Funktion, verwendet ist.

7. Fahrzeugsicherungseinrichtung nach einem der Ansprüche 1 bis 6, weiter dadurch gekennzeichnet, daß eine Mehrzahl von fahrzeugseitigen Geräteeinheiten (2) parallel zum Bestimmen der jeweiligen Ist-Berechtigungsinformation aus einer empfangenen Benutzercodeinformation und zum Vergleichen derselben mit der Soll-Berechtigungsinformation sowie zum vergleichsabhängigen Erzeugen einer Nutzungsfreigabeinformation eingerichtet ist.

8. Fahrzeugsicherungseinrichtung nach einem der Ansprüche 1 bis 7, weiter dadurch gekennzeichnet, daß ein Schließsteuergerät des Fahrzeugs eine fahrzeugseitige Geräteeinheit der Sicherungseinrichtung bildet.

9. Fahrzeugsicherungseinrichtung nach einem der Ansprüche 1 bis 8, weiter dadurch gekennzeichnet, daß
   - die jeweils gesendete Benutzercodeinformation (M) eine fahrzeug- und eine schlüsselspezifische Identifizierungsinformation beinhaltet und
   - die Identifizierungsinformation einer empfangenen Benutzercodeinformation in einer fahrzeugseitigen Geräteeinheit (2) vorab auswertbar ist, wobei der Nutzungsberechtigungs-Prüfvorgang nach Erkennung nichtberechtigender, gesendeter Identifizierungsdaten abgebrochen wird.

10. Fahrzeugsicherungseinrichtung nach einem der Ansprüche 1 bis 9, weiter dadurch gekennzeichnet, daß
   - mehrere berechtigende benutzerseitige Schlüsseleinheiten für ein Fahrzeug vorgesehen sind, die unterschiedliche Urbildwertfolgen (m_j) senden,
   - die gesendeten Benutzercodeinformationen (M) jeweils eine Schlüsselidentifizierungsinformation (ID_j) beinhalten und
   - in jeder beteiligten fahrzeugseitigen Geräteeinheit (2) für jede Schlüsseleinheit eine spezifische Soll-Berechtigungsinformation in einen Speicher (16), der mit Hilfe der Schlüsselidentifizierungsinformation adressierbar ist, einspeicherbar und aus diesem auslesbar ist.

Hierzu 1 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 44 11 449 C1
Int. Cl.[6]: B 60 R 25/00
Veröffentlichungstag: 16. März 1995